TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ARMIN IRAQI

DEVELOPING IT CONTROLS TESTING FOR ENTERPRISE ENVIRONMENT

Master of Science thesis

Examiner: prof. Jarmo Harju
Examiner and topic approved by the Faculty of Computing and Electrical Engineering
Novermber 5th, 2014

ABSTRACT

ARMIN IRAQI: Developing IT Controls Testing for Enterprise Environment
Tampere University of Technology
Master of Science Thesis, 47 pages
December 2014
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Professor Jarmo Harju

Nowadays enterprises are highly dependent on Information Technology (IT) for accomplishing their objectives. In order to try to ensure that IT is aligned with the business objectives, an enterprise should ensure that it has effective IT controls for supporting its IT environment. Therefore, for checking the effectiveness of its IT environment, the enterprise's IT environment is tested against the enterprise's IT controls. So it is correct to state IT controls testing plays a crucial role in trying to ensure that the IT environment of an enterprise is reliable for achieving the business goals.

But it should be kept in mind that IT controls testing is a very challenging process. For instance, some of the challenges are the work effort required to complete the test, the speed of the test, accuracy, etc. Another challenge is the high cost of IT controls testing. During the accomplishment of the thesis, it has been observed that to solve the above-mentioned challenges, a lot of enterprises rely on Computer-Assisted Audit Techniques (CAAT) tools available in the market.

After analyzing some of the most popular and widely used CAAT tools, it has been found out that such tools are helpful, but they are having their own challenges. For instance, they are not able to address all the requirements of IT controls testing. Furthermore, CAAT tools are capable of performing specific tasks; they are not able to address all the issues related to IT controls testing. Their main challenge is the insufficient use of existing Enterprise Resource Planning (ERP) data.

The solution for having an effective IT controls testing process could be the appropriate use of enterprise's existing ERP data which is of high quality. In fact, the data should be measured and analyzed appropriately, and it should be mapped to the IT controls in a correct way. Actually, it might be challenging and even expensive to implement such a system, but if such system is implemented once, and it could be used for several years with minor updates, then it would be worthy to implement it for a reliable IT controls testing in an enterprise environment.

PREFACE

This master thesis is based on comprehensive research on IT controls testing. The target of the thesis is to develop IT controls testing in enterprise environment. Major part of the thesis is based on my work experience. Due to confidentiality issue, I am not allowed to expose the name of the company, even though the thesis is not done in association with any company.

In addition, first and foremost I would like to express my sincere gratitude to my supervisor, Professor Jarmo Harju, whose expertise, patience, understanding and motivation, added considerable value to my master thesis. Furthermore, I appreciate his friendly support that helped me to manage my stress throughout the accomplishment of my master thesis.

Furthermore, I would like to use this opportunity to offer my sincerest appreciation to my dear friend and information security colleague, Erik Taavila, who supported me throughout the thesis with his immense knowledge in almost any IT security and compliance related field. In fact, I am certain that without Erik's support, it would be impossible to complete my master thesis. Besides, I must also acknowledge my other colleagues, Pekka Erma and Jari Österberg, for teaching me the building blocks of IT security and compliance. I highly appreciate Erik Taavila, Pekka Erma and Jari Österberg for their positive influence on my professional career path.

I must express my gratefulness to my amazing friends, Amir Shokouhifard, Alaaeddin Loulou, Malihe Soleimani, Farid Mehrabkhani and Mieraisan Mieraidihaimu, for their support throughout my master's degree program. In fact, I am grateful to them.

I would also like to extend my appreciation to my dear friends, Behrouz, Tuomo, Rose, Arman, Emad, Iida, Jenni, Ehsan, Masoud, Lassi, Daniel, Behnam, Behnum, Nazanin, Kaveh, Mehrnaz, Hanna and Saeed for helping me to stay positive and focused.

I wish to express my appreciation to my beloved family, mum, dad, Arian, Behrouz, Behzad, Ali Reza, Nastaran, Nico, Niki, Esko, Tiina and Pia. I am grateful to my dear parents for supporting me throughout my entire life. And I am especially grateful to my twin brother, Arian, who is of great value to me. Arian has always inspired me by his diligence, discipline and motivation.

Finally, I would like to express my deepest gratitude to the beautiful love of my life, Annette, who encouraged and motivated me throughout my studies.

Armin Iraqi

Helsinki, 3.11.2014

"Happiness Only Real When Shared" – Christopher McCandless

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1 Motivation

With the expansion and development of Information Technology (IT), almost each and every governmental, industrial, financial, educational and many other similar entities became more dependent on IT in many different aspects. For example, governments deploy IT for various public services, military forces rely on IT in the battlefield, hospitals depend greatly on IT for better healthcare services, and almost every business enterprise relies on IT for one reason or another. Therefore, it is correct to claim that IT influences almost every aspect of the modern life, and its role is crucial.

Similar to many other technologies, in addition to advantages that IT provides for such entities, there exist also various disadvantages. In fact, due to large-scale dependency on IT, a lot of entities have been experiencing series of destructive and negative issues in their environments (Vicente & Mira da Silva, 2011). For instance, in the case of a bank, due to a poor IT architecture, if the bank fails to provide a particular IT service, such as online transaction, the customers of the bank will not be able to perform their desired functions. As a result, the bank will lose its customers; therefore, the bank might experience a crisis.

Furthermore, IT is being used in order to accomplish illegal and malicious actions, such as stealing credit card numbers, using telephone systems illegally, stealing trade secrets of business corporations, modifying contents of governmental websites for political causes, committing extortion, spying on governments to obtain strategic information, etc., (Harris, 2010). In addition to external threats, internal threats are considered to be a key factor as well. For example, during maintenance at a data center of an enterprise, if equipment is damaged, loss of data is possible. And if there is no suitable backup procedure in use, the enterprise will fail to proceed with service delivery.

By doing a simple and quick internet research, various security breaches that occurred in the recent years could be observed. And these security breaches had devastating effects on various businesses, governments and individuals. For example, Stuxnet, a malware that infected the software of Iran's uranium-enrichment site, resulted in hindrance of Iran's nuclear program (Kushner, 2013). Another example could be the case of eBay, where the hackers stole names, email addresses, postal addresses, date of births and phone numbers of 233 million users (Williams, 2014).

Moreover, the complexity is still increased when the nature of these threats changes. In the Data Breach Investigation Report which is made by Verizon Communications Inc.,

it is mentioned that in the year 2013, there has been "*a transition from geopolitical attacks to large-scale attacks on payment card systems"* (Data Breach Investigation Report, 2014). Therefore, any business enterprise or a similar entity with a large and complex IT environment, and with limited budget, has an appropriate justification to be worried about its IT environment; the IT environment that is affecting the strategic objectives of the above-mentioned organizations either directly or indirectly.

As a matter of fact, with respect to the examples of security breaches discussed in the previous paragraph, and due to the problems caused by these breaches, the trust in the affected corporations has been faded (Vicente & Mira da Silva, 2011). Therefore, such issues need to be prevented or mitigated for providing appropriate level of assurance for any entity (Racz, Weippl, & Bonazzi, 2011).

Considering internal and external threats, besides deploying security countermeasures, enterprises are concerned about other factors as well. The issues and challenges of effectively managing an organization's IT services and resources are of key concern for executive management and the Board in many organizations. Therefore, for many organizations, main concerns are development of methods and practices for the solution of operational planning and optimization of IT processes (Krey, Harriehausen, & Knoll, 2011). And due to the fact that businesses have been experiencing an exceptional chain of IT incidents, focus on organization's IT Governance, Risk and Compliance (GRC) has increased (Vicente & Mira da Silva, 2011). As a result, importance of IT controls rises as well, considering that IT controls are subset of IT GRC.

According to (Puspasari, Hammi, Sattar, & Nusa, 2011), IT GRC refers to organization-wide governance, risk, and compliance that tries to ensure that an organization acts appropriately in accordance with its risk appetite, internal policies, and external regulations through the alignment of processes , strategy, technology and people, thereby improving efficiency and effectiveness. If performed right, IT GRC activities will certainly develop effectiveness of organization's IT environment. And this is directly proportional to the improved value of many internal functions of the organizations (Vicente & Mira da Silva, 2011).

Thus, a key element to support that IT is streamlined with the objectives and strategies of the organization is the internal IT controls. IT controls benefit companies in assessment and improvement of their IT environments. In an organization, in order to check if the applications, services and processes are reliable and functioning effectively, they will be tested against IT controls (IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, 2006). Therefore, an IT control testing is vital for any enterprise that has an IT environment, particularly the enterprises with large IT environments.

1.2 Objective

The objective of this thesis is to perform a comprehensive research on challenges of the existing IT controls testing processes in enterprise environments, and to develop IT controls testing for such environments. The main concern of this thesis is to address crucial factors of IT controls testing, for instance, increasing the rate, accuracy and speed of IT controls testing, and decreasing the work effort and cost of IT controls testing.

1.3 Structure of Thesis

This thesis includes four chapters; Introduction, Background, Analysis and Development, and Conclusion. Chapter one includes the motivation behind this thesis, objective and structure of the thesis. In Chapter two, IT GRC, IT controls, COBIT 4.1 framework, Information Technology Infrastructure Library (ITIL) and IT controls testing are comprehensively explained. The third chapter includes explanation and description challenges and targets of IT controls testing, Enterprise Resource Planning (ERP), Computer-Assisted Audit Techniques (CAAT) and existing CAAT tools. Finally, Chapter four covers the conclusion of this thesis.

2. BACKGROUND

This chapter includes an elaboration of the main concepts related to IT controls testing. First, IT GRC will be explained thoroughly. IT GRC will be explained in such a way that all the three entities, namely, governance, risk and compliance will be addressed in a separate way. Second, the concept of IT controls will be described. In addition, Control Objectives for Information and Related Technology (COBIT) will be comprehensively explained. Furthermore, concepts such as Information Technology Infrastructure Library (ITIL) and Enterprise Resource Planning (ERP) will be illustrated.

2.1 Introduction to IT GRC

Due to the importance of effective governance to the enterprises, the concentration on IT has been increased accordingly. As a matter of fact, many large enterprises are global, and due to this reason they are having their departments scattered in various geographical locations. Hence, IT could be of great value for providing appropriate governance. And for achieving such systematized governance throughout the enterprise, in any governance, risk and compliance initiative, IT GRC has an essential role (Under Control; Governance Across the Enterprise, Chapter 7).

Moreover, in order to understand the term IT GRC, primarily, it is essential to comprehend governance, risk and compliance. Therefore, governance, risk and compliance are defined separately. In addition to the definition of risk, governance and compliance, these terms are defined in association with IT as well.

In addition, in Figure 1 (Adams;Ruiz;& Rivera, 2013), the relationship of the key entities of IT GRC is illustrated. As it can be observed, strategy, goals and objectives, policies and procedures, and structures and processes belong to governance section. Furthermore, compliance part addresses controls, laws and regulations, activities, etc. Finally, risk section, includes risk identification, risk analysis, risk monitoring, etc.

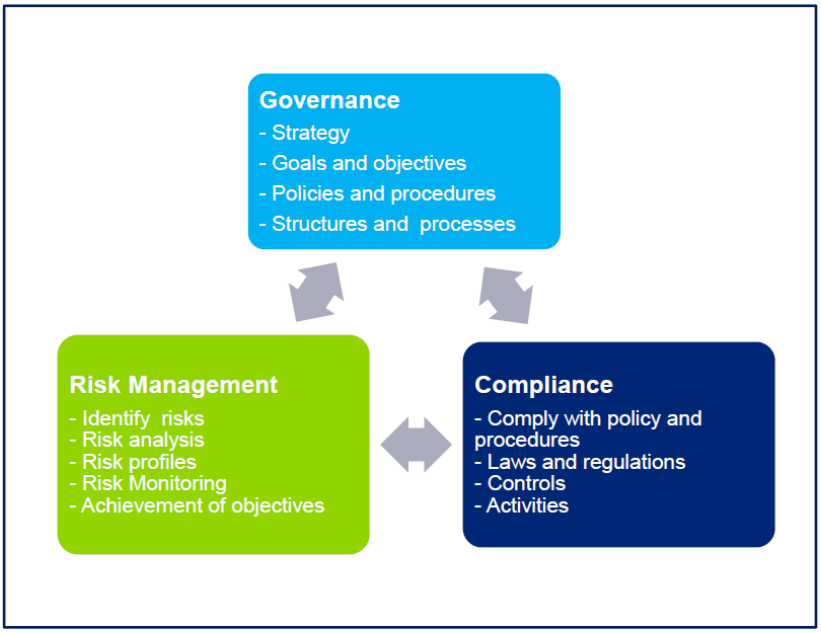

Figure 1: IT GRC

2.1.1 IT Governance

With respect to the pervious paragraph, initially, it is important to know the meaning of governance. According to (Under Control; Governance Across the Enterprise, Chapter 2), *"governance is the leadership, organizational structures and processes that help ensure that an organization's functions sustain and extend its strategies and objectives. Put more simply, it is the culture, policies, procedures and controls that help ensure a company will meet its business goals.*"

Since, the focus of this thesis is on IT GRC, therefore, it is necessary understand the meaning of IT governance. Referring to (Niemann, 2006), for defining IT governance, first, it should be noted that in an enterprise, board of directors and the executive management are responsible for IT governance. Furthermore, IT governance is vital subset of enterprise governance, which includes policies, procedures and processes to align IT with the strategies and objectives of the enterprise. In conclusion, IT governance aims to accomplish the following:

- IT effectiveness
- IT reliability

For more clarity, it is important to understand the focus areas of IT governance. According to (IT Governance Institute, 2007), there are five IT governance focus areas, which are mentioned and explained as the following:

- Strategic alignment

    - This focus area concentrates on alignment of IT and business. Moreover, strategic alignment defines, maintains and validates IT value proposition. Therefore, strategic alignment aims to align IT operations with the enterprise's operations.
- Value delivery
    - Value delivery deploys delivery cycle for accomplishing the IT value proposition in order to help to ensure that IT supports enterprise's strategies and objectives, by focusing on cost optimization and proving the essentiality of IT.
- Resource management
    - The main objective of resource management is the optimization of knowledge and infrastructure. It is about investment which is optimal, and it is also about appropriate management of critical IT resources. The critical IT resources are applications, information, infrastructure and people.
- Risk management
    - For managing risks in an appropriate manner, five factors are highly considered to be essential. It is required that key and senior enterprise officers are aware of risk. Second, there should be a clear comprehension of how much risk the enterprise is willing to take, in other words, the senior officers should clearly know their enterprise's risk appetite. Furthermore, the legal and regulatory requirements should be understood, that is, it is required that the compliance requirement should be clear enough for the enterprise. Moreover, significant risks to the enterprise should be transparent and finally, risk management responsibilities should be set in the enterprise.
- Performance measurement
    - The main principle of performance measurement is to monitor and track the key functions regularly, for instance, implementation of strategy, completion of projects, use of resources, service delivery etc.

2.1.2 IT Risk

Risk is defined as a possible problem or the prospect of loss. And the risk associated with IT is called IT risk. IT Risk is measured as the product of the likelihood of occurrence an event and impact of the event (Ginzberg & Moulton, 1990).

Moreover, in an enterprise, when it comes to risk, management of risk is of great concern. An enterprise deploys the process of risk management for the following purposes:

- Determining willingness of accepting risk
- Identifying risks to its strategies and objectives
- Developing plan for mitigating risk

Thus, risk management plays a crucial role in an enterprise. And the goal of risk management is value creation for the company and loss reduction (Under Control; Governance Across the Enterprise, Chapter 2).

In fact, enterprises are highly dependent on IT; and poor IT architecture can adversely affect the strategies and objectives of an enterprise. Thus, IT presents risks to the enterprise, and the risk associated with IT, is termed as IT risk (Ginzberg & Moulton, 1990).

2.1.3 IT Compliance

According to (Chen;Yoon;Frenz;& Compres, 2011), *"Compliance in a literal sense is an action, state or fact in accordance with or meeting rules or standards,* and according to (Under Control; Governance Across the Enterprise, Chapter 2), *"compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations, as well as internal corporate policies, procedures, and controls."*

In recent years, the demand for IT GRC has increased enormously. And this is mainly because, legal and regulatory authorities are concerned about the social values such as privacy, safety and accessibility, specially, when it comes to enterprises performing IT business practices for delivering services and products. As a result, due to laws and regulations, such authorities impose requirements on enterprises. Therefore, to address the compliance risks, enterprises integrate their service delivery and product development with organizational frameworks and infrastructures (Breaux;Antón;Boucher;& Dorfman, 2009). Due to dependency of enterprises on IT, and in order to be compliant to regulatory obligations and requirements, IT compliance is introduced. IT compliance is compliance with focus on IT (Chen;Yoon;Frenz;& Compres, 2011).

2.2 IT GRC in Depth

After understanding the terms IT governance, IT Risk and IT Compliance, it is needed to explore the term IT GRC in depth. It should be noted that in an enterprise, risk and compliance are managed throughout the enterprise. But due to the fact that IT plays a crucial role as a supporting function for fulfilling the strategies and objectives of an enterprise, IT GRC becomes particularly important (Under Control; Governance Across the Enterprise, Chapter 7).

Therefore, inappropriate IT GRC within an enterprise is considered as a threat for the enterprise (Under Control; Governance Across the Enterprise, Chapter 7). For example, consider an organization with various number of services which are all IT based; for instance, financial services, human resource services, sourcing services, supply chain services, etc., and in case of such enterprise, with plenty of IT services, there is high possibility of IT incidents. If there is no proper IT GRC in place, then an appropriate change management control is not used, thereby, there is no sense of prioritization for

resolving the incidents. As a result, an incident which is urgent, and is supposed to have a huge impact on the business, might be resolved when it's too late, and an incident which is not critical at all, might be handled immediately, which does not require immediate action. As a result, even though, the enterprise might have skilled employees and necessary means to tackle the issues, but due to the fact that within the enterprise there is no appropriate IT GRC in use, there will be lack of governance of IT risks and issues, consequently, obstructing the enterprise from reaching its main objectives and goals.

Now that the meaning and importance of IT GRC is explained, and for more clarity to understand how IT GRC operates in large enterprises, it is necessary to look at the IT GRC roles. Similar to executive management and board of directors who own and manage the business processes, IT Compliance Team is responsible for trying to ensure that the IT procedures, processes and systems of the enterprise are in compliance with regulatory mandates, internal policies and industry requirements. This team, works as a link between business unit and IT department (Under Control Governance Across the Enterprise, Chapter 7).

In fact, IT Compliance Team has a good level of understanding IT risks. IT Compliance Team monitors IT business processes. It is important to consider that IT Compliance Team is not responsible for operating controls; hence, it functions as an objective testing body to be leveraged by other teams or departments, such as internal audit, to provide an understanding of operation of IT controls. For example, the IT Compliance Team provides instructions and guidelines for the auditors to test particular IT controls (Under Control Governance Across the Enterprise, Chapter 7).

In general, IT Compliance Team monitors and measures the processes and state that if IT is in line with risk appetite of the enterprise that is defined by the higher authorities of the enterprise, such as board of directors and executive management. Or in case, IT is deviated from the strategies and policies of the enterprise, the IT Compliance Team can report the deviation. In this regard, for daily business processes, IT Compliance Team has to controlling ownership responsibilities. In fact, IT Compliance Team helps the business unit executive to understand if IT related processes are done correctly, in a right time and for the right purpose

To be clearer, the IT Compliance Officer of the enterprise monitors compliance related tasks, such as measuring risks (their urgency and impact) and reporting deviations to business unit executive. In conclusion, the functions and performance of IT Compliance Team is directly proportional to the executive leadership's comprehension of how IT decisions affect the compliance posture, risk tolerance levels, and strategies and objectives of the enterprise (Under Control; Governance Across the Enterprise, Chapter 7).

2.3 IT Controls; a Subset of Enterprise's Internal Control

The main focus of this section is IT controls. But due to the fact that IT controls is a subset of internal control, primarily, internal controls will be described. After grasping the concept of internal control, focus will be diverted on IT controls.

2.3.1 Introduction to Internal Control

In an enterprise, the Board of Directors is responsible for the trying to ensure that the enterprise's functions, procedures and processes are streamlined with the strategies and objectives of the enterprise. In order to meet this target, deployment of an appropriate GRC is required. For supporting this initiative, effective internal controls should be in place. They are aware that the enterprise must meet the legal and regulatory obligations; therefore, they are highly concerned to meet such legal commitments, because they are also aware that failure in fulfilling the obligations will make the enterprise prone to stiff penalties, which they want to avoid certainly. And in order to reduce the associated risk, internal controls are implemented (Humphreys, 2008).

2.3.2 Definition of Internal Control

In the regard to accounting and auditing, internal control is a procedure or process for supporting an enterprise to achieve its objectives in such a way that the enterprise is in compliance with regulatory mandates, internal policies and industry requirements. It is correct to state that internal control is directly associated and involved with controlling risks to an enterprise (Sawyer, 2012).

As a matter of fact, there are a lot of definitions for internal control. One of the reliable definitions is made by the Committee of Sponsoring Organizations (COSO). According to widely internationally used framework, which is termed as the (COSO, 2013), internal control is generally defined as a set of processes affected by an enterprise's Board of Directors, executive management, and other personnel, intended to support the enterprise in achieving its goals relating to operations, compliance and reporting. Based on COSO's definition for internal control, internal control is having five components; the five components and their main concept are described as the following:

- Control Environment
    - The culture of enterprise is set by the control environment. And this control environment affects the awareness of its employees; therefore, this component is the basis for all the other internal control's components.
- Risk Assessment
    - Another key component is risk assessment; having a foundation for how the risks are addressed and managed. It is highly essential to manage the risks, so that the enterprise is able to achieve its objectives. Managing the risks is done by risk identification and analysis of relevant risks.

- Information and Communication
    - In an enterprise, for the employees to be able to perform their tasks and to carry out their responsibilities, they require information and communication. This component includes the systems and processes that are needed for identification, capture and information exchange in a procedural and timely manner.
- Control Activities
    - The fourth component is the control activities. The control activities includes policies and procedures that try to ensure management and business
- Monitoring
    - And finally, in order to evaluate, assess and check the quality of internal control performance, the fifth component exists, and that is monitoring (Securities and Exchange Commisions, 2007).

2.3.3 IT Controls

Prior to defining the meaning of IT controls, it is highly crucial to comprehend the reason behind the need for the deployment of IT controls. Therefore, in the following paragraphs, the motivation behind deployment of IT controls is described.

Perhaps, in the recent years, there has been constant occurrence of various security breaches and incidents associated with various enterprises. And it is mainly due to the fact that IT controls are neglected. According to (PriceWaterhouseCoopers, 2014), "*Organizations do not adequately address employee and insider vulnerabilities, nor do they assess the security practices of third-party partners and supply chains*". Even though relevant authorities have prompted the enterprises to meet the legal and regulatory requirements, but still if the enterprises are not having an appropriate implementation of IT controls, the occurrence of security breaches and incidents obstructing the enterprises from achieving their goals is inevitable (Yu;Seo;& Kim, 2013).

According to the internal control improvement strategy issue report of finance IT (S.H.Hong, 2011), the reason for 60 percent of the security accidents is the employee of the enterprise. It also states that large enterprises are more vulnerable to the internal threats. This shows that no matter how strong security technologies are used, without an appropriate IT controls, enterprises are not only facing the risk of not being in compliance with regulatory and legal mandates, but also they are obstructed by the internal threats for achieving their targets. For instance, studying the "Key Findings from the 2014 US State of Cybercrime Survey", illustrates that how the employees of an enterprise could make the enterprise prone to security threats. For instance, Figure 2 (PriceWaterhouseCoopers, 2014) depicts the causes and consequences of cybercrime committed by insiders in United States of America, in the year 2014.

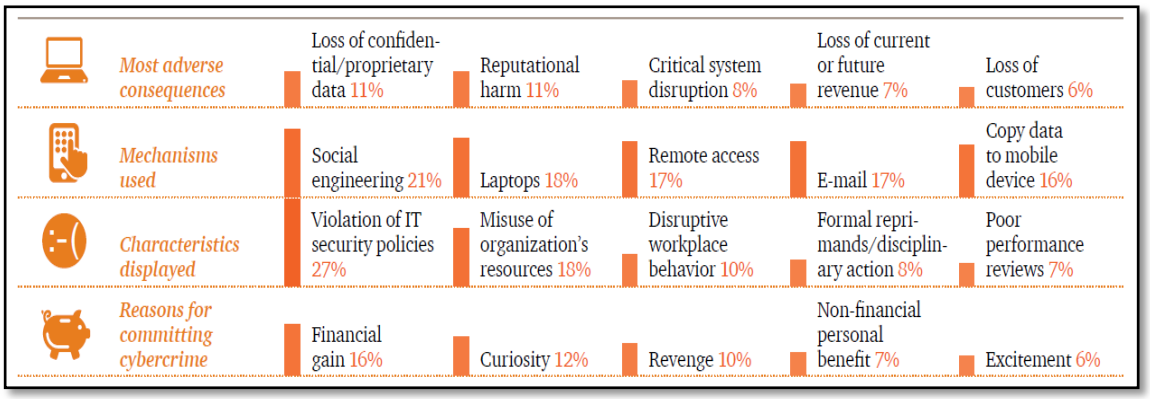

Figure 2: The causes and consequences of cybercrime committed by insiders

Another example that helps to understand the internal threat is the case Bank of America confidential information leakage. This event also has occurred by a former employee of Bank of America, whose role was program developer (Yu;Seo;& Kim, 2013). Therefore, it is highly essential to take the internal threats serious, for the enterprise to run business effectively, efficiently and consistently. And in order to so, a crucial element is IT controls.

At this point, where the importance of IT controls is realized, it is important to understand the meaning of IT controls. As it is mentioned earlier, IT controls are a subset of internal control. Besides, for the enterprise to have an effective IT governance, Board of Directors and executive management requires the implementation of controls for all IT processes by the IT Compliance Team. The IT controls help to achieve to manage IT adequately, in such a way that IT is streamlined with the strategies and objectives of the enterprise (IT Governance Institute, 2007).

Furthermore, IT controls are categorized into two groups. The categories are IT general controls and IT application controls. The following is brief explanation of IT general controls and application controls (IT Governance Institute, 2007):

- IT general controls are concerned with IT services and processes. Examples of IT general controls are:
    - Change management
    - Security
    - Computer operations
    - Systems development
- IT application controls are concerned with business process applications. Examples of IT application controls are:
    - Completeness
    - Validity
    - Accuracy
    - Segregation of duties
    - Authorization.

In addition, it is important to note that a control could be used or ignored an enterprise based on several factors. For instance, in an enterprise, there might be no need for putting in place a control, because the enterprise does not find that particular control relevant to its business objectives. Or maybe even the cost of implementing the control is higher than the risk associated with that control. In fact, these are just of the factors that might affect control selection in an enterprise.

2.4 COBIT

Section 2.4 highly depends on COBIT 4.1 (IT Governance Institute, 2007). A big amount of the information provided in this section is either based on the COBIT 4.1 documents, or it is copied from the COBIT 4.1 document without any alteration. This is because, the information provided by COBIT 4.1 is highly reliable, and the best approach to understand the COBIT 4.1 framework is to go through the unaltered information retrieved from COBIT 4.1.

2.4.1 Motivation for Using COBIT 4.1

It is observed that enterprises have high dependency on IT. Therefore, efficient, effective and reliable IT governance is needed. And this shows that enterprises are concerned about alignment of IT and business objectives. In addition, the enterprises are aware of the fact that IT governance is a vital factor in the achievement of enterprise's objectives (Hussain & Siddiqui, 2005). As aligning IT and business objectives in an enterprise is an essential success parameter (Parvizi;Oghbaei;& Khayami, 2013), deploying a reliable framework is essential.

As a matter of fact, IT resources should be managed by a set of grouped processes so that necessary information for the enterprise to meet its goals and objectives is provided. And it is challenging for the enterprise to determine how to control IT so that the enterprise's needs are fulfilled by IT. The enterprise also faces the challenge of managing risks associated with IT, securing its IT environment, and more importantly achieving its business objectives that is dependent on IT. Therefore, for the management of the enterprise to be able to provide a reasonable level of assurance to achieve the enterprise's business objectives, and to address undesired events, it should define critical goal of implementing policies, procedures and plans. And for such definition, control objectives are needed (IT Governance Institute, 2007).

For this purpose, COBIT is used, and in this thesis, the focus is on COBIT 4.1. And this is because COBIT 4.1 has proved to be effective and reliable, and it is a highly developed framework. And with respect to all the above-mentioned facts, it is indicated that COBIT 4.1 is a trusted framework for aligning IT environment with business objectives.

Now that for this thesis COBIT 4.1 is chosen, in order to explore in depth the definition and fundamental aspects of COBIT 4.1, the focus will be on the source published by Information Systems Audit and Control Association (ISACA). Most of Section 2.4 is based on the aforementioned source. And this is because; COBIT 4.1 is created by ISACA (IT Governance Institute, 2007).

2.4.2 Definition and Advantages of COBIT

COBIT framework is a framework that supports the managers to align IT and business objectives by bridging the gap between the above entities with respect to control requirements, technical matters and risks. And it helps the managers to make the stakeholders understand how IT as a function supports the enterprise in the achievement of its business objectives and strategies. Briefly, the fundamental principle of COBIT framework is management of IT resources by relying on IT, in order to achieve IT goals that are required by an enterprise to accomplish its business objectives.

As it can be illustrated in Figure 3 (IT Governance Institute, 2007), the basic principle of COBIT framework supports the enterprise in the achievement of its business objectives. COBIT framework helps the achievement of business objective to be enhanced by providing the information that the enterprise relies on. In addition, COBIT framework delivers information that the enterprise needs for IT investment, IT management and controlling IT resources, and this is done by deploying a structured set of processes. As a result of the above-mentioned facts, service delivery is accomplished in accordance to enterprise information.

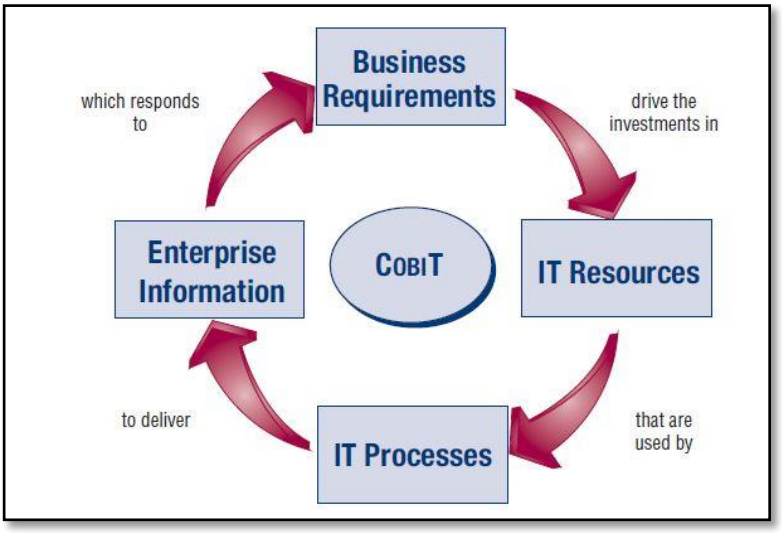

Figure 3: Basic COBIT principle

A more detailed relationship of IT goals and business goals from COBIT 4.1 perspectives could be achieved by referring to Figure 4 (IT Governance Institute, 2007). This figure depicts the importance of business goals for IT, IT goals, IT architecture, etc. in

achieving the objectives of the enterprise. It also illustrates the importance of entities, such as IT resources, IT processes, governance requirements, information services, etc. in achieving the enterprise's goals.

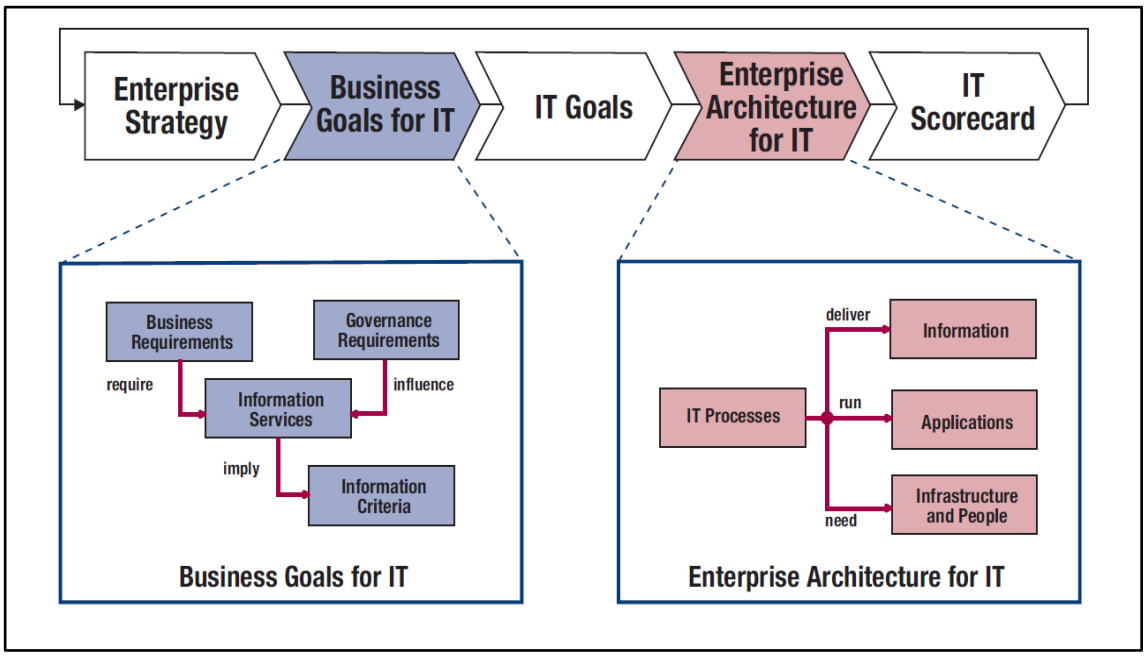

Figure 4: Business and IT Goals

In addition, COBIT provides the opportunity to develop clear policies and good industry practices for IT control in an enterprise. It is important to note that COBIT is kept up-to-date and consistent with others standards and guidance. As a result, when it comes to IT good practices and IT governance, COBIT acts as an integrator. Moreover, COBIT helps in comprehension and management of advantages and disadvantages associated with IT. Therefore, since COBIT is having a high level and business-oriented process structure, it provides an end-to-end understanding of IT, and this assists the enterprises in making decisions about IT. It is important to note that The COBIT framework is crucial part of IT governance implementation.

Mainly, for IT governance implementation, the process assessment capability based on COBIT maturity models is highly important for an effective implementation of IT governance in an enterprise. The COBIT maturity modelling helps to identify gaps in capability of critical IT controls and processes. In addition, it also helps to illustrate the identified gaps to the management. Plus, the desired IT controls and processes maturity level could be achieved by setting action plans in such a way that the target level is obtained.

In fact, COBIT framework acts as a supporter of IT governance that tries to ensure the following:

- Alignment of IT and business

  - It is important to comprehend the business goals, as well the IT goals. The objectives of business and that of the IT should be aligned obtaining a common target.

- IT enables business
  - The role of IT in IT dependent enterprises is considered to be a functional role. In fact, IT should be used to achieve the business objectives. There is no point, if an enterprise relies on an IT environment, which is not facilitating the business.

- Benefits of IT are maximized
  - COBIT framework tries to ensure the efficient and reliable use of IT in an optimal manner. When an enterprise invests a huge amount of input IT for running its business, for sure, it is important to get the maximum benefit out of its IT environment.

- Responsible use of IT resources of the enterprise
  - In an enterprise, it is very important to use the IT resources in a responsible way. And this is because IT resources are important assets of an enterprise. For example, if the IT resources are not used responsibly, it is possible that the IT cost increases, which in turn adversely affects the enterprise.

- Appropriate handling and management of risks associated with IT
  - COBIT tries to ensure risk management by putting control objectives in place. For instance, COBIT 4.1 includes a control termed as "Assess and Manage IT Risks", which involves risk assessment, risk remediation, etc. This control will be elaborated later in this chapter.

Moreover, COBIT benefits IT governance by setting IT based on a business focus, and it provides an understandable picture of what IT does. In addition, with respect to the processes, it tries to clearly define the roles and responsibilities of the employees. Besides, it bridges the enterprise with third parties and regulators. Plus, it creates a common language among the stakeholders, and finally, it addresses the IT control environment's requirements.

Finally, by referring to the Figure 5 (IT Governance Institute, 2007), a better general understanding of COBIT framework could be achieved. The diagram illustrates the relationship of the COBIT components in a very organized and structured method. For instance, it depicts how important is the relationship of IT Goals and Business Goals. In fact, it can be concluded that ignoring IT goals, will obstruct an IT dependent enterprise from achieving its business goals.

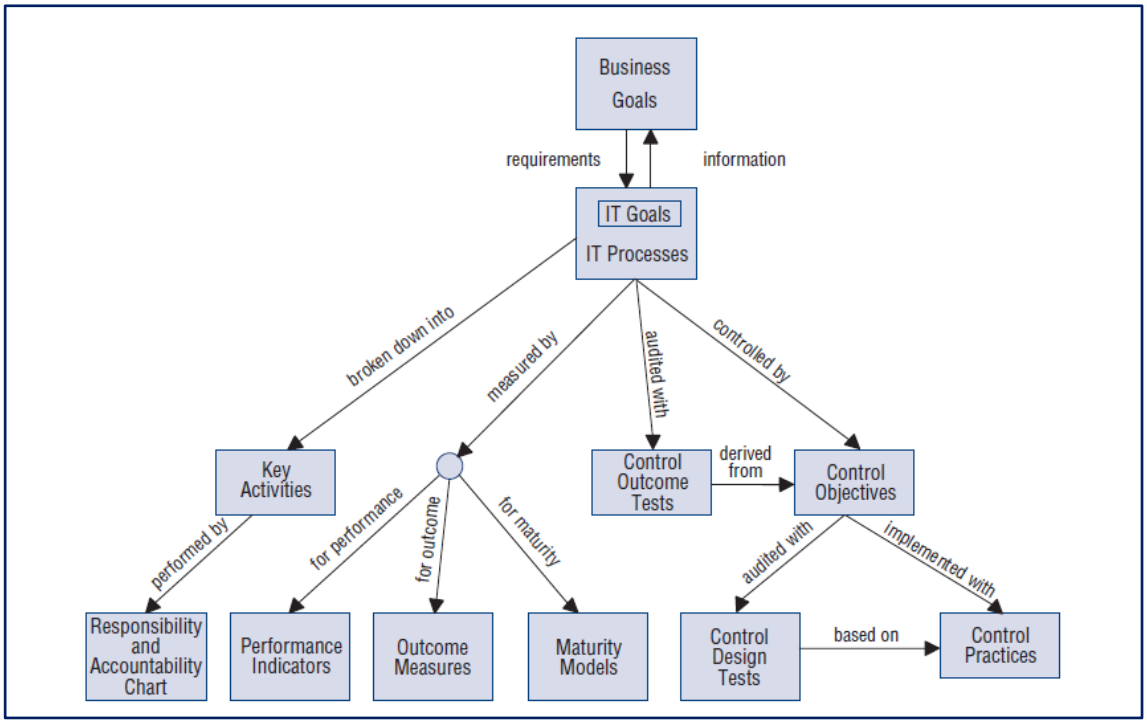

Figure 5: Interrelationships of COBIT components

2.4.3 COBIT 4.1 in Depth

The COBIT framework divides IT into four domains and 34 processes. These domains and processes are in line with entities such as plan, build, run and monitor, thereby providing an end-to-end insight of IT environment of the enterprise. It should also be considered that there are four IT resources identified in COBIT. The IT resources are applications, information, infrastructure and people, and these IT resources are of vital value for process success. And Figure 6 (IT Governance Institute, 2007) depicts how IT business goals affect the management of IT resources by processes for achieving its objectives.

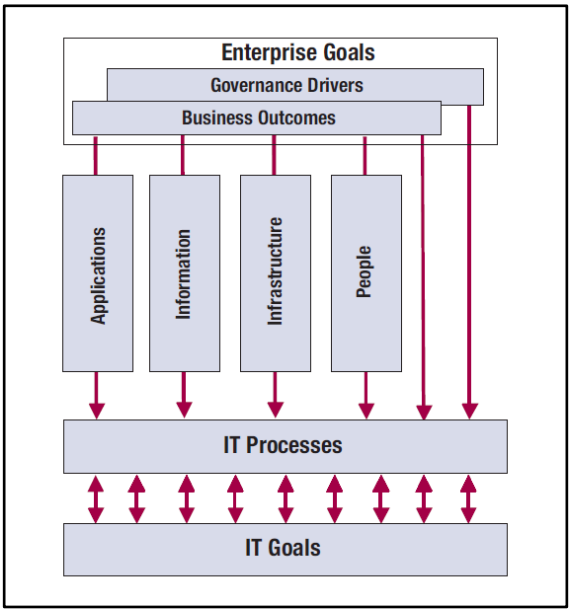

Figure 6: Managing IT resources to deliver IT goals

For effective IT governance, activities and risks associated with IT environment need to be managed, and managing these is of great concern. This is commonly under the responsibility domains of plan, build, run and monitor. In COBIT 4.1, these domains are termed as:

- **Plan and Organize (PO)**
  - Plan and Organize domain includes strategy and tactics. This domain is concerned with identifying how IT can affect achieving business objectives in the best possible way. Moreover, it addresses alignment of IT and business strategy, optimized use of IT resources, understanding IT objectives, risks management and appropriateness of IT quality.
- **Acquire and Implement (AI)**
  - This domain acts as a solution provider. In fact, it is necessary to identify, develop and acquire IT solutions to understand the IT strategy. In addition, it is also important to implement these solutions and integrate them into the business processes. This domain is concerned about new projects. For instance, it controls if the new projects are delivered in a timely manner, or if the new projects are fulfilling the business requirements, etc.
- **Deliver and Support (DS)**
  - This domain is concerned with service delivery, service support, security management, service continuity, etc. To summarize, it is concerned with delivery of needed services. This domain addresses if IT service delivery is prioritized based on business needs, and it is also concerned with IT costs optimization, productive and safe use of IT systems and information security.
- **Monitor and Evaluate (ME)**

- This domain monitors and evaluates all the IT process regularly. The intention of this regular assessment is to check the quality of IT processes, and to check if the processes are in compliance with control requirements. This domain typically addresses measuring IT performance for problem detection, and it checks if the management ensure the effectiveness and efficiency of the controls, information security, etc.

Another key aspect of COBIT framework is the maturity models. COBIT's maturity model helps to measure IT performance of the enterprise, identify the status of the enterprise, enterprise's target, and the required growth path. COBIT 4.1 includes 0 to 5 maturity scale, which is represented in Figure 7 (IT Governance Institute, 2007):

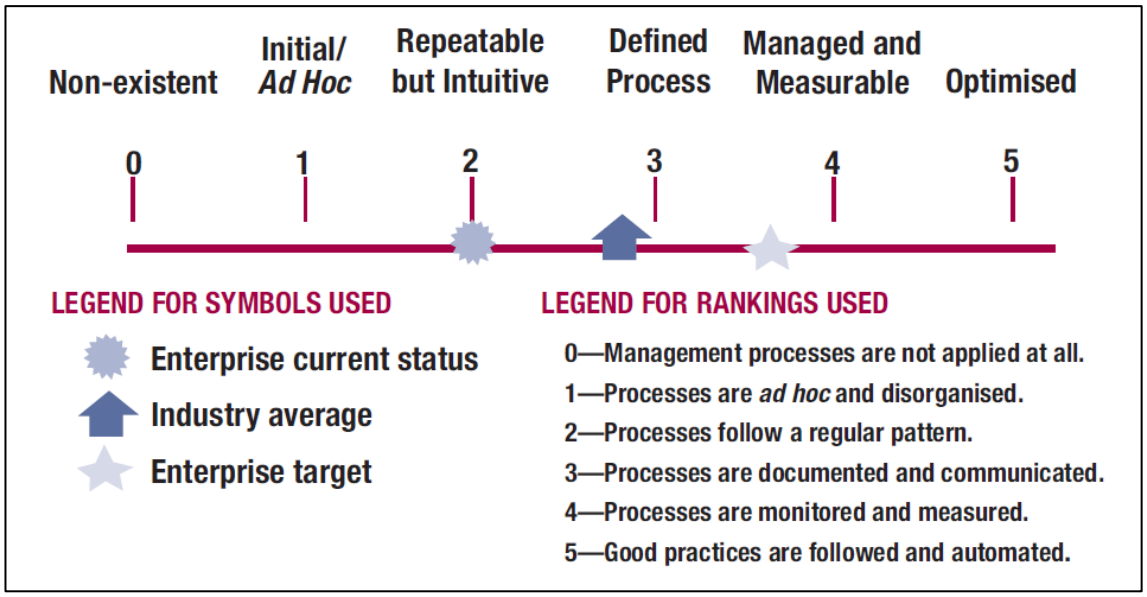

Figure 7: Graphic representation of maturity models

0 Non-existent: This states that the enterprise does not have any recognized process. In fact, according to the enterprise, there is no issue for being addressed.

1 Initial/Ad Hoc: In this case, the enterprise has noticed that there are some issues that require to be addressed. But they lack any recognized for process for addressing for addressing the issues. Instead, an ad hoc approach by individuals is practiced for solving the issues or even on a case-by-case basis.

2 Repeatable but Intuitive: Maturity level 2 indicates that processes are developed for addressing issues, and procedures are followed by different individuals. In fact, there is no standard procedure or training or communication, therefore, the way the problems are addressed highly depends on the individual's knowledge. This approach makes the enterprise prone to errors.

3 Defined Process: In this case, standard procedures exist and they are documented. In addition, the standard procedures are communicated through trainings. It is compulsory that the procedures must be followed, but chance of detecting deviations is low.

4 Managed and Measurable: Maturity level 4 is a good state f addressing issues. In fact, in this case, enterprise's management monitors and measures compliance. The compliance is monitored and measured with standard procedures, and actions are taken if a process does not appear to be in order. Processes are improved constantly and automation and tools are in place, but they are used is a limited and fragmented way.

5 Optimized: This is highest level of maturity where the process developed to a level of good industry practice. The refining of processes is done based on the results of regular improvement and maturity modelling with the other enterprises. IT plays a key role in integrating and automating the workflow. In addition, IT provides tools for improving quality and effectiveness, and this will help to enterprise to adapt quickly.

2.4.4 COBIT's Control Objectives

COBIT 4.1 includes control objectives for 34 processes, and all these processes need controls, since, the controls are designed and implemented in such a way that a reasonable level of assurance to meet business objectives is achieved. The controls help the prevention, detection and correction or mitigation of undesired events. To grasp an idea of how the COBIT 4.1 IT processes and IT controls are functioning, some of the most important COBIT 4.1 processes that are widely used in many enterprises, such as assess and manage IT risks, manage changes, ensure systems security, and ensure compliance with external requirements are described. Actually, one example from each of the four domain areas of COBIT 4.1 is explained. In addition, in accordance to the provided COBIT 4.1 processes, COBIT 4.1 based IT controls that are vital in enterprises are explained. Therefore, each example includes a description of the process and relevant IT control that is used during the process of IT controls testing.

Example 1:

Process: Assess and Manage IT Risks (Plan and Organize)

This process of COBIT 4.1 framework is included in the first domain of the framework. The process addresses the creation and maintenance of a risk management framework. In addition, it includes common and agreed level of risks associated with IT, mitigation strategies and residual risks. In this case, if there is any potential impact on the objectives of the enterprise due to unplanned event, the cause undergoes risk identification, risk analysis and risk assessment. Furthermore, in order to minimize the residual risk to an accepted level, risk mitigation strategies are in place. The risk assessment's result if understandable for the stakeholders and the result are expressed in financial terms. This enables the stakeholders to align IT risk to an acceptable level of risk tolerance.

The control over this process is “assess and manage IT risks”, and its focus areas are as the following:

- IT Risk Management Framework
- Establishment of Risk Context
- Event Identification
- Risk Assessment
- Risk Response
- Monitoring & Maintenance of a Risk Action Plan.

Control: Assess and Manage IT Risks

Figure 8 illustrates how an enterprise could create IT controls based on COBIT 4.1 framework. In this example, the control includes four control requirements and corresponding test scripts (answer, evidence and deviation field are intentionally left empty).

Control	Control Requirement	Test Script	Answer	Evidence	Deviation
Assess and Manage IT Risks	A formal IT risk management framework should exist.	Does the enterprise has a formal IT risk management framework?	N/A	N/A	N/A
	Risk assessment should be performed quarterly.	Is risk assessment performed quarterly?	N/A	N/A	N/A
	Risk responce process must be developed and maintained.	Does the enterprise has a formal risk response process?	N/A	N/A	N/A
	Risk response actions must be approved by the service owners.	Are the risk response actions approved by the service owners?	N/A	N/A	N/A

Figure 8: Assess and Manage IT Risks

Example 2:

Process: Manage Changes (Acquire and Implement)

Manage changes belongs to the second domain of COBIT 4.1 framework and it addresses formal and controlled management of all changes, including emergency changes and patches, relevant to applications and infrastructure with the production environment. Changes relating to processes, procedures, systems and services should be logged, assessed and authorized. All these should be done before implementation phase. In addition, post implementation reviews must be performed. This provides assurance of mitigation of risks that are negatively affecting the integrity and stability of the production environment.

The control over this process is “manage changes”, and its focus areas are as the following:

- Change Standards and Procedures
- Impact Assessment, Prioritisation and Authorisation
- Emergency Changes
- Change Status Tracking and Reporting
- Change Closure and Documentation.

Control: Manage Changes

Figure 9, illustrates the use of manage changes control in an enterprise. In the following figure several control requirements and relevant test scripts are provided (answer, evidence and deviation field are intentionally left empty).

Control	Control Requirement	Test Script	Answer	Evidence	Deviation
Manage Changes	A formal change management process should exist.	Does the enterprise has a formal change management process?	N/A	N/A	N/A
	Changes should be tracked by using an online ticketing tool.	Is there ticketing tool in place for tracking changes.	N/A	N/A	N/A
	Changes must be approved by the change manager.	Are the changes approved by the change manager?	N/A	N/A	N/A
	Emergency changes must follow the emergency plan.	Are the emergency changes following the emergency plan?	N/A	N/A	N/A
	The resolution information of the changes must be in English.	Are the resoultion information in English.	N/A	N/A	N/A
	Priority 1 changes must be classied as critical.	Are the priority 1 changes classified as critical.	N/A	N/A	N/A

Figure 9: Manage Changes

Example 3:

Process: Ensure Systems Security (Deliver and Support)

This process of COBIT 4.1 framework belongs to the third domain of the framework, which is called deliver and support. It addresses the necessity of maintaining information integrity and IT assets protection through security management process. Establishment and maintenance of IT security roles and responsibilities, procedures, policies and standards are included in this process. Moreover, security monitoring and periodic testing, implementing corrective actions for known security vulnerabilities and incidents are also include in the process of security management. The process states that in order to minimize the impact of security weaknesses and incidents, effective security management is required to protect all IT assets.

The control over this process is “ensure systems security”, and its focus areas are as the following:

- Management of IT Security
- IT Security Plan
- Identity Management
- User Account Management
- Security Testing, Surveillance and Monitoring
- Security Incident Definition
- Protection of Security Technology
- Cryptographic Key Management
- Prevention, Detection and Correction of Malicious Software
- Network Security
- Exchange of Sensitive Data.

Control: Ensure Systems Security

Figure 10 is a very basic example of an IT control. As it can be seen, in accordance with the control, there are some control requirements and test scripts (answer, evidence and deviation field are intentionally left empty).

Control	Control Requirement	Test Script	Answer	Evidence	Deviation
Ensure Systems Security	A formal IT security management process should exist.	Does the enterprise has a formal IT security management process?	N/A	N/A	N/A
	A formal IT security plan that includes business, risk and compliance requirements should exist.	Does the enterprise has a formal IT security plan that includes business, risk and complinace requirmeents?	N/A	N/A	N/A
	Appropriate identity management process and tool(s) should be deployed for maintaing user identities and access rights.	Are all the users and their activties uniquely identifiable? Are the access rights in line with the defined and documented business needs and job requirements? Are the access rights by the user management? Are the access rights approved by the systems owners? Are the access rights implemented by security responsible person? Are the user identities and access rights maintained in a central repository?	N/A	N/A	N/A

Figure 10: Manage Changes

Example 4:

Process: Ensure Compliance with External Requirements (Monitor and Evaluate)

This process belongs to the last domain of COBIT 4.1 framework. Ensure compliance with external requirements process tries to ensure compliance with laws, regulations and contractual requirements, through an effective review process. The process includes compliance requirements identification, response optimization and evaluation, compliance verification, and integrating IT compliance report with the enterprise's business report.

The control over this process is "ensure compliance with external requirements", and its focus areas are as the following:

- Identification of External Legal, Regulatory and Contractual Compliance Requirements
- Optimisation of Response to External Requirements
- Evaluation of Compliance With External Requirements
- Positive Assurance of Compliance
- Integrated Reporting.

Control: Ensure Compliance with External Requirements

Figure 11, shows briefly how the ensure compliance with external requirments control is used in an enterprise. It is a very important control with regard to IT compliance (answer, evidence and deviation field are intentionally left empty).

Control	Control Requirement	Test Script	Answer	Evidence	Deviation
Ensure Compliance with External Requirements	Enterprise relevant international laws, regulations and other external requirements must be identified quarterly.	Are the enterprise relevant international laws, regulations and other external requirements identified on a quarterly basis?	N/A	N/A	N/A
	Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.	Are the IT policies, standards, procedures and methodoligies reviewed and adjusted in such a way that legal, regulatory and contractual requirements are addressed and communicated?	N/A	N/A	N/A
	Every year, IT Compliance Team must conduct trainings ofr all the IT employees of an enterprise to create awareness about compliance.	Does the IT Compliance Team conduct compliance training on a yearly basis?	N/A	N/A	N/A

Figure 11: Ensure Compliance with External Requirements

2.5 Information Technology Infrastructure Library (ITIL)

When it comes to the topic of IT controls, it is important to understand the concept of IT Service Management (ITSM). Therefore, in this section, first the ITSM is explained briefly, and then the focus is on ITIL.

Nowadays, ITSM is of high concern internationally. And this is mainly because; enterprises in highly competitive business environments are worried about their key business aspects, such as efficient and cost effective service delivery. Hence, enterprises need the support of ITSM to reach their objectives (Yao & Wang, 2010). In this regard, ITSM is defined as the implementation and management of quality IT services, and it is done by IT service management, performed by IT service providers through people, process and IT (Hanna, 2011).

Perhaps, in addition to issues mentioned in the previous paragraph, due to the complex and distributed IT environments the enterprises are relying on, approach towards a best practice for management of IT services in such a way that IT is in line with the business objectives of the enterprise is inevitable (Yao & Wang, 2010). In this regard, in many enterprises across the world, reliable IT service management is done by using the ITIL approach. And ITIL is de facto standard for managing IT in enterprises across the world (Long, 2008).

ITIL consist of a set of best practice in a unified and organized approach. This cohesive set of best practice is drawn from public and private sectors across the world (Key Benefits of ITIL). It provides identifying, planning, delivering and supporting IT services to the enterprise's business (What is ITIL?).

2.6 IT Controls Testing

For the enterprises it is very crucial to have an appropriate IT environment, so that they succeed in achieving their business goals. The role and importance of IT controls in order to have effective IT governance is also explained. Now it is important to focus on a very significant section of this thesis; IT controls testing.

In fact, IT controls testing is a function that supports audit objectives of IT environment (Pathak, 2005). IT controls testing is the process of evaluating and assessing IT performance of an IT environment by collecting evidences through different means and evaluating the evidences (Radovanović;Radojević;Lučić;& Šarac, 2010).

In addition, IT controls testing process determine if the enterprise's IT environment is in line with business objectives, uses IT resources appropriately, possesses information

security, etc. For more clarity, objectives of IT controls testing are summarized as the following (Pathak, 2005):

- Tests reliability, accuracy and appropriateness of the IT processes
- Checks if the IT processes are in compliance with regulatory and enterprise's requirements
- Tests secure and safety aspects of the enterprise's IT environment against internal and external threats
- Ascertains the accuracy of information processed in the enterprise
- Checks the reliability, effectiveness and efficiency of IT resources.

For grasping a better comprehension of IT controls testing, referring to Figure 12 is helpful. The following figure is a basic example of how an IT control that is tested in an enterprise.

Control	Control Requirement	Test Script	Answer	Evidence	Deviation
Manage Incidents	A formal incident management process should exist.	Does the enterprise has a formal incident management process?	Yes, formal incident management process exists.	Link	N/A
	Incidents should be tracked using a ticketing tool.	Does the enterprise has a ticketing tool for tracking incidents?	Incidents are tracked using a ticketing tool.	Link	N/A
	Incidents should be handled according to the incident manegement process.	Are the incidents handled accroding to the incident management plan?	Most of the incidents are handled according to the incident management process, but in 2 cases deviations have been observed.	Ticket number 7834734 and 8948394	Out of 15 samples tested, 2 samples have not followed the incident management process.
	Incident resoultion information must be in English.	Are the incident resoultion information in English?	Yes	Link	N/A
	Priority 1 and priority 2 incidents should be classified as critical.	Are the priority 1 and 2 incidents classified as critical?	Yes	Link	N/A
	Incidents should be reviewed regulary (acording to the formal incident management process).	Are the incidents reviewed regulary (acording to the formal incident management process).	Yes the incidents are reviewed regularly.	Link	N/A

Figure 12: Manage Incidents

In the above figure, it can be observed that several control requirements exist. And in accordance to the requirements, test scripts are included as well. In this test, five questions are asked from the employee who is responsible for a particular service. The tester, interviews the interviewee, observe the evidences, and fill the fields accordingly.

In fact, IT controls testing in this case could be accomplished in different ways. A poor case could be that the tester only relies on the interviewee's claims, for example, the interviewee says that everything is okay, and the tester marks that everything is okay,

without checking the evidences. Or might be the other way around, for example, the tester does not refer to the interviewee's claims, and he/she just fills the fields based on the evidences, which is also a poor method of testing. An appropriate method would be interviewing, and correlating the claims of the interviewee with the evidences.

2.7 Enterprise Resource Planning (ERP)

For the purpose of IT controls testing, the use of existing Enterprise Resource Planning (ERP) data is crucial. Hence, it is important to understand ERP. Therefore, ERP and its importance are explained in this section.

Enterprise Resource Planning (ERP) is business management software. ERP is usually used a suite of integrated applications. In an enterprise, ERP is used for various functions, such as data collection, data storage, data management and data interpretation.

In the enterprises, the main purpose of the above-mentioned functions are product planning (cost), service delivery, manufacturing, sales and marketing, management of inventory, shipping, payment, etc.

In fact, ERP is of highly value when it comes to viewing core business processes in an integrated way. And this is because, and often this approach is done in real-time, using the existing common databases of the enterprise. In addition, ERP systems of the enterprises perform functions, such as tracking of resources (raw materials, financial status, purchase orders, etc.). As a matter of fact, the ERP applications share data across different departments of the enterprise (IT, human resource, supply chain, finance, sales, etc.) that provide the data (Rouse, 2014). In this regard, in the enterprises, ERP eases data and information flow between all core business functions, and it manages connections to outside stakeholders (Bidgoli, 2004).

In the Figure 13 (SAP Enterprise Resource Planning (ERP), 2013), a very simple understanding of the role of ERP in an enterprise, and its relationship with the other entities could be comprehended. For instance, in the picture, it is seen that all the important and major entities of an enterprise, such as supply chain management, project management, customer relationship management, human resources, etc., are connected to ERP. The following picture briefly explains the key role of ERP in an enterprise.

Figure 13: Enterprise Resource Planning (ERP)

Hence, ERP system of an enterprise is considered as an important organizational tool. And this is because of the fact that it integrates various organizations functions, such as production, transaction, etc. Moreover, ERP systems functions on various components of an enterprise, such as network, computer hardware, databases, information repository, etc. (Khosrowpour, 2006).

3. CHALLENGES, ANALYSIS AND DEVELOPMENT

3.1 Challenges and Targets of IT Controls Testing

An effective IT controls testing is a challenging process due to several factors. These factors are geographically scattered enterprises, decentralized management process, multiple IT systems, complex IT environment, lack of skilled personnel to focus on IT controls, decentralized compliance efforts, limited technological backing for documentation, testing and reporting (compliance activities), high dependency on manual control procedures due to lack of technologies to support automated controls and enterprise's limited budget. To summarize, the main challenges of the existing IT controls testing are huge amount of manual work, inaccuracy, low frequency, and low coverage (usually only the critical systems are tested). However, it should be also noted that if all these challenges are tackled, it means that the process becomes very expensive, and cost is a very serious factor in the enterprises (PwC, 2008). In addition, attention needs to be paid to IT controls testing approaches that are not only outdated, but they are not utilizing the capabilities of testers in the best possible way. Besides, the potential capabilities of the enterprise's IT Enterprise Resource Planning (ERP) are not utilized in an appropriate style. Therefore, target for an ideal IT controls testing, best information set should be available (Schultz;Ruehle;& Gehrke, 2014).

Each of the above-mentioned challenges is having their own complications. For instance, according to (Under Control; Governance Across the Enterprise, Chapter 7), manual work involves human interference, paper work and decision making. And this means that manual testing is prone to severe challenges. It is expensive, because as it involves more human activities, therefore, it requires more personnel. Since there is human intervention, there is always a chance of human error. In addition, they lack the scalability factor, especially in case of large enterprises. For example, an IT control such as "manage changes" might require a particular personnel's approval for 100 changes prior to their release in the enterprise's production environment throughout a year. In this case, maybe the control works appropriately. But if in an enterprise 100 manual approvals are needed per month, this control is definitely not accomplishing its task in an appropriate manner.

Therefore, for reducing such problems, automation of controls is required. Actually, it is easier to monitor such controls, since they are automated. In addition, because of their automated nature, they do not involve much of human intervention; as a result, devia-

tion from policies is decreased or detected through the use of relevant technologies. Moreover, by implementing and deploying automated controls, with the enterprise growth, the work effort of the personnel will not increase. And this is because, large and complicated tasks could be managed in a way similar to small and simple tasks by using automated controls (Under Control; Governance Across the Enterprise, Chapter 7).

But again, as it is mentioned earlier, justifying the expense of such controls is challenging (PwC, 2008).But then in case of identification of risk associated with manual controls, expensive automated controls could be justified using the argument discussed. But of course, it is up to the enterprise's risk appetite and risk tolerance to decide whether they want to avoid the risk, mitigate it, accept it or transfer it. In addition, enterprises are concerned with cost benefits, as a result of the above-mentioned considerations; they can decide to either ignore automation of controls, or partially use such controls, or to completely make use of automated controls. Therefore, it can be concluded that, by investing in technologies that could support automation of IT controls, less time is consumed, work effort is decreased, thereby, cost is decreased with this regard, and the control's effectiveness is increased (Under Control; Governance Across the Enterprise, Chapter 7).

3.2 Computer-Assisted Audit Techniques (CAAT)

In many cases, techniques used by a tester to test IT system is not computer assisted. Hence, CAAT is something really superior. As it has been mentioned earlier, in most of the enterprises, IT plays a vital role. In fact, in an enterprise, maybe a few numbers of processes are not IT dependent. Therefore, it is correct to state that testing without relying on IT is not an appropriate option. Especially, by considering that most of the processes related information is stored in the IT system of the enterprise, it is not an appropriate decision to ignore the use of IT for testing purposes. Therefore, CAAT could be defined as deployment of IT tools by the tester to perform testing, in this case IT controls testing. CAAT are classified into various categories. For example, data analysis software, network security evaluation software/utilities, operating system security evaluation software/utilities, database management system software/utilities, software and code testing tools, etc. (Sayana, 2003).

Since, data analysis software is the main category of CAAT, it is described furthermore. Data analysis software is the main category of CAAT. It is also referred to as audit software. Under this category, the products with general purpose are called general purpose audit software. In addition, it is also known as generalized audit software. One of the important capabilities of this software is the data extraction from sources, commonly used files, database system tables, etc. Due to this reason, the data analysis software could be used during testing on different platforms for almost any application or service. Furthermore, data analysis software is able to accomplish various types of analysis on data, for instance, data analysis software can accomplish various queries on data. In

addition to data queries, data analysis software can perform stratification of data, extracting samples, identifying missing sequence, analyzing and calculating in a statistical method. It is also having the ability to perform operations, such as merging files and tables (combining and joining). In fact, with respect to different products or versions, there exist different features, which are of great value when it comes to IT controls testing (Sayana, 2003).

3.3 Existing CAAT Tools

3.3.1 BWise® Internal Audit (BWise IA) software solution

BWise is an international enterprise GRC software leader. It is a Nasdaq company, which provides solutions for the GRC needs of hundreds of customers, worldwide, across all industries. And it is having strong heritage when it comes to business process management. For instance, BWise has been quoted by Independent research firm Forrester as the "Leader in GRC Platforms" in their Q1 2014 report.

BWise delivers a promising and integrated GRC tool, and this is with respect to its strong heritage in business process management. The BWise GRC platform provides beneficial features such as tracking, measuring and managing significant organizational risks in an integrated system.

In fact, enterprises which are concerned with maintaining a balance between their performance and risks associated, could rely on BWise, since, it has the features to address organizational risks. In this regard, BWise supports enterprises to be in control of balancing the performance of their enterprise and the risks associated. In addition, by comprehending risks, BWise support the enterprises to achieve the following objectives:

- Increasing business accountability
- Strengthening financial efficiency
- Consolidating strategies
- Improving operation efficiency
- Maximizing performance
- Complying with regulations, such as Sarbanes-Oxley, ISAE3402/SAS-70, ISO standards, European Corporate Governance Codes, etc. (BWise, 2014).

In order to analyze BWise, the focus is on BWise IA solution, which is completely relevant to this thesis. As a matter of fact; BWise claimed that it released a new solution for internal audit.

As it has been mentioned frequently in this thesis, currently, there is high pressure on the enterprises with regard to legal and regulatory requirements, vulnerability to fraud, and complex business environment, BWise has come up with some promising statements. For instance, BWise claimed that ensuring appropriateness of design and per-

formance of controls; testers are capable of detecting fraud and mitigating risks in an ongoing way. BWise use the data available in an enterprise, as a result, by continuous monitoring and intelligent testing value is derived. Hence, work effort in the enterprise is decreased.

In fact, trying to ensure that an enterprise obtains its objectives, and protecting it against fraud by managing risks in an appropriate way are very challenging for the testers. Thereby, BWise IA assists the testers to address such challenges. This support is seen in testing process, merged with various features.

According to (ProQuest, 2014), the important and new features promised by BWise IA are mentioned in the following:

-*"Full audit planning, scheduling and time-keeping*

-*Off-line audit: synchronize work when connected again*

-*Online and off-line testing of controls*

-*Define annual audit plans, including individual audits and allocation of auditors*

-*Work-paper management, recording of findings and issues*

-*Store audit evidence, in one single, centrally managed secure audit environment*

-*Manage the audit workflow and create audit reports*

-*Audit analytics: continuous monitoring integrated in audits"*.

The CTO and founder of BWise claims that by integrating audit analytics in their GRC platform, BWise has turned into the leading advanced testing platform globally. In addition, BWise Audit Analytics provides the secure extraction of data. For instance, data is extracted securely from SAP or Oracle sources, and thereby, adds data into the testing process. In this case, testers can set rules for analysis; hence, they can perform data analysis in an advanced way. And this feature benefits the testers to concentrate on high risks due to the high level automated testing process (ProQuest, 2014).

3.3.2 Oracle Enterprise GRC Manager – Fusion Edition (Enterprise GRC Manager)

Importance of improving enterprise's IT controls for meeting regulatory mandates has already been discussed in this thesis. In order to meet the requirements of increasing demand of enterprises to improve the quality and effectiveness of their compliance program, Oracle introduced Enterprise GRC Manager.

The main promises of the Oracle Enterprise GRC Manager are briefly provided in the following (Oracle, 2009):

- Supports the enterprise to fulfil for real-world requirements
- It has a common platform
- In addition to common platform, it has modular application
- It is secure
- Oracle Enterprise GRC Manager provides dynamic user experience
- It seamlessly fits in the enterprise's IT environment
- It provides a comprehensive management of risk
- It improves the enterprise's performance
- It performs in-context risk significance analysis
- Provides models for risk treatment/mitigation
- It decreases the compliance cost
- It decreases the compliance work effort
- It performs test scoping based on risk
- Provides management of audit testing
- It minimizes redundant testing
- It improves risk coverage
- It provides consolidate view of issues
    - Significance
    - Level of risk exposure
    - Remediation time
- It integrates IT controls monitoring
- It provides real-time GRC reports
- It manages GRC in a sustainable method.

In summary, it can be concluded that Oracle Enterprise GRC Manager supports enterprises to perform enterprise-wide compliance management, develop a bottom up/top down risk management platform, increase productivity through automation of GRC process, ensure transparency provides traceability compliance and risk activities, and reduces the cost of GRC management.

3.3.3 ServiceNow IT Governance, Risk and Compliance

ServiceNow is an IT cloud company that transforms IT across global enterprises. To be elaborate, IT transformation in global enterprises is done by ServiceNow by automating IT services and managing the across the enterprises. ServiceNow provides the following features to the enterprises (ServiceNow, 2014):

- Single system of record for IT
- Automation of manual tasks
- Standardization of processes
- Consolidation of legacy systems.

ServiceNow provides an extensible platform. Therefore, enterprises have the ability to create custom applications that address the IT service model of the enterprise to the service domains of the enterprise both internally and externally.

For meeting the regulatory and legal mandates, such as SOX, ITIL, COBIT, etc., ServiceNow introduced ServiceNow IT Governance Risk and Compliance (IT GRC). ServiceNow IT GRC automates the enterprise critical process of measuring and managing compliance. The first step taken by ServiceNow IT GRC is the documentation of policies. Then it performs the task of risk definition in context of compliance, and for designing IT controls that is needed for policy enforcement and risk mitigation. In the further steps, IT GRC is deployed for schedule IT controls testing. In fact, it is used for evidence collection, failure identification and remediation. In the end, for IT controls testing, information is extracted from the service management process as evidence.

As a matter of fact, every enterprise must adhere with legal and regulatory mandates. These mandates are required by the authoritative sources. Hence, as discussed earlier, the enterprises are completely aware of the consequences that they might have in not meeting the requirements. Especially the enterprises that are operating in complex regulatory environment are highly concerned with such matters. The enterprises are having challenges in being compliant with the above-mentioned mandates. For instance, appropriate IT compliance management is complex, time-consuming and costly. And in this regard, ServiceNow claims that ServiceNow IT GRC provides beneficial features that are briefly explained in the following (ServiceNow IT Governance, Risk and Compliance, 2014):

- ServiceNow IT GRC relies on a single source
    - It automatically extracts information from service management process in the ServiceNow as compliance evidence
    - Uses data certification for validating the information extracted from ServiceNow Configuration Management Database (CMDB)
- ServiceNow IT GRC reduces the IT compliance complexity
    - Uses document and knowledge management capabilities for managing publication and version control of policies
    - ServiceNow dashboards provides assessment and remediation reports
- ServiceNow IT GRC streamline IT controls testing
    - Creates a process for IT control validation and testing by using audit definitions
    - Reduce the work load of evidence collection
    - Decrease the time consumption for evidence collection
- ServiceNow IT GRC performs risk mitigation
    - Supports IT compliance by policy enforcement
    - Provides automatic remediation tasks in case of findings.

To grasp a better understanding of ServiceNow IT GRC environment, briefly the following Figure 14 (ServiceNow, 2014) is illustrated. As it is illustrated, different and important entities are appropriately present in the tool. For instance, there are separate sections such as controls, controls test, remediation, audit, authoritative sources, observations, administration, etc. And in the right sector of Figure 14, mapping of various entities needed for IT controls testing is shown. For instance, in the following figure, the relation between control objective of SOX to other entities, such as emergency change request procedure, IT policies and procedures, COBIT 4.1, etc., is mapped and illustrated.

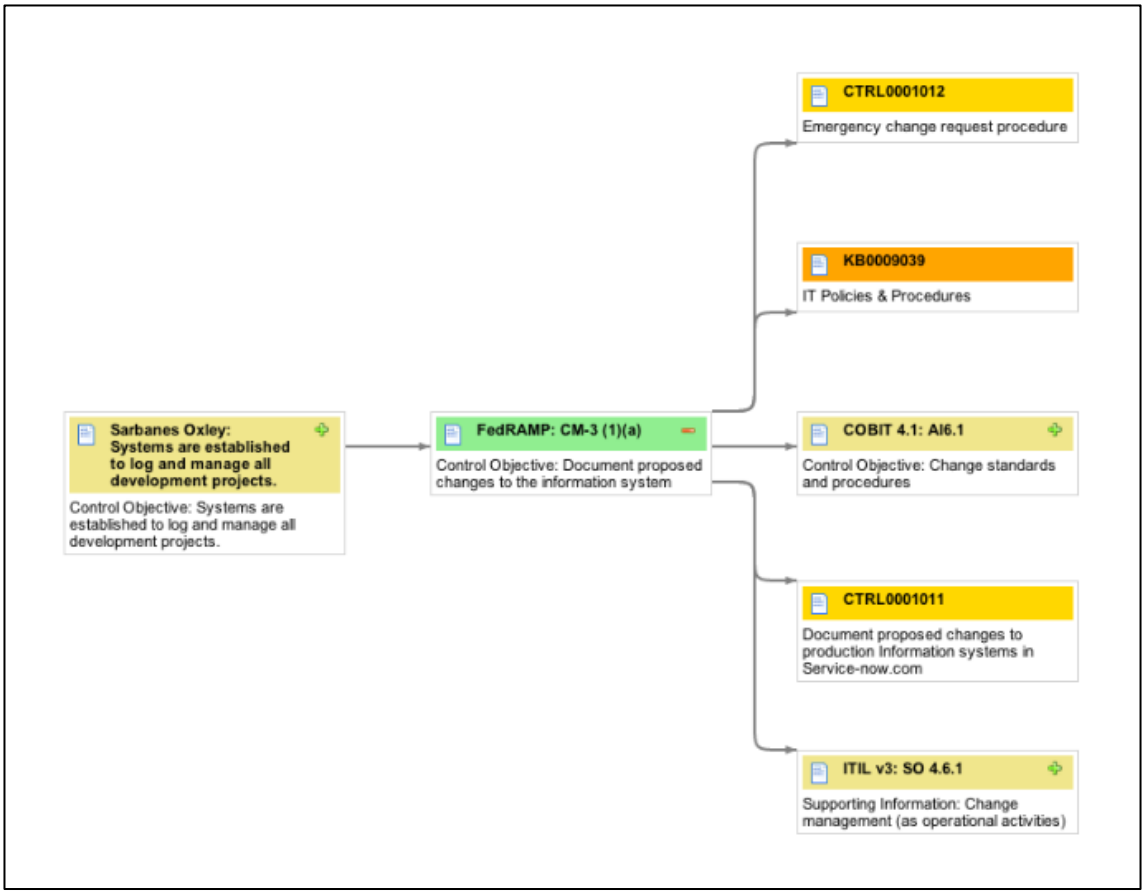

Figure 14: ServiceNow IT GRC Environment

3.4 Symantec Control Compliance Suite

Symantec is one of the largest software companies in the world. The main deliverables of Symantec are security, storage and systems management solutions.

The enterprises are look forward to effective alignment of priorities with regard to IT operations, IT security and IT compliance. In this regard, Symantec claims that the Control Compliance Suite delivers risk visibility and business-aware security to the enterprises. The Control Compliance Suite is capable of automating assessments in a continuous manner. In addition, it is capable of providing a view of security controls and the

associated vulnerabilities in a unified way. Moreover, the Control Compliance Suite provides the enterprises with various capabilities, such as hardening of data center, prioritizing security remediation, enabling the migration to the software-defined data center in a secure manner, and supporting continuous assessing for monitoring for cyber security.

In fact, Symantec Control Compliance has various beneficial characteristics. It is a scalable, modular, and comprehensive tool for automation of security and compliance assessments. It consists of seven independent modules, which are mentioned in the following section:

- Symantec Control Compliance Suite Policy Manager
- Symantec Control Compliance Suite Risk Manager
- Symantec Control Compliance Suite Standards Manager
- Symantec Control Compliance Suite Vulnerability Manager
- Symantec Control Compliance Suite Virtualization Security Manager
- Symantec Control Compliance Suite Assessment Manager
- Symantec Control Compliance Suite Vendor Risk Manager.

For this thesis, two of the modules are chosen arbitrarily for analysis purposes. The two modules are Symantec Control Compliance Suite Vendor Risk Manager and Symantec Control Compliance Suite Virtualization Security Manager (Symantec Control Compliance Suite).

3.4.1 Symantec Control Compliance Suite Vendor Risk Manager

Symantec Control Compliance Suite Vendor Risk Manager has the capability to automate various numbers of tasks. In fact, it automates tasks associated with vendor risk management process. For instance, it automates tasks such as variable scoping, creating assessments, developing standards, collecting evidence, analyzing risk evidence, tracking, etc (Symantec Control Compliance Suite, 2014).

Briefly explaining, the main features of Symantec Control Compliance Suite Vendor Risk Manager are as the following:

- By automating security and compliance assessments, it manages risk associated with third-party service providers (business process service providers, third party application developers, cloud service providers, etc.).
    - For example, it uses centralized and web-based repository for managing vendor assessment process and evidence collection.
    -
- It performs automatic calculation of vendor risk scores, thus, enhancing the process of risk scoring in context of risk areas. In fact, Control Compliance Suite Vendor Risk Manager categorizes evidence sources and their associated components in different risk areas, such :

    - as data risk
    - operational risk
    - brand risk
    - financial risk.
- It provides advanced compliance reports and analytics, which can be great help for supporting risk remediation, enterprise planning activities and operational alignment.

In addition to the above-mentioned, it also provides some other beneficial features, which are elaborated in the following:

- Identification and assessment of risks associated with third parties
- Provides an effective vendor risk management procedure to the auditors and the customers
- Effective and accurate communication of risk information to the executives in short period of time
- Manage incidents related to third party services
- When it comes to addressing and responding to security breaches by the third parties, it supports the standards and internal processes
- Assess risk across the entire enterprise.

3.4.2 Symantec Control Compliance Suite Virtualization Security Manager

Symantec Control Compliance Suite Virtualization Security Manager provides the opportunity for the enterprises to make use of virtualization without being worried about compliance issues and enterprise reputation. The Control Compliance Suite Virtualization Security Manager provides strong and powerful control features. It allows the isolation of compliance relevant virtual assets. In addition, Control Compliance Suite Virtualization Security Manager limits to and from the isolated compliance relevant virtual assets. It provides operation control for the system administrators for fulfilment of their requirements, without making other applications of the same infrastructure prone to risk (Control Compliance Suite Virtualization Security Manager, 2012).

Control Compliance Suite Virtualization Security Manager has granular access control capability. It reduces access to accounts that are privileged. Moreover, it is also handling the access to the virtual assets. It deploys two-factor approval cycle, thereby; an additional security layer is used for key actions. In addition, it has the capability of automating regular assessment of both security and configuration settings for the virtual environment. It has the capability to log successful actions, failed actions and changes. This provides the testers in depth data for addressing their requirements as well as regulatory requirements.

It is important to note that the merging of the above-mentioned control features improves the overall security of the enterprise. In addition, it reduces risk. For instance, it reduces the risk associated with unplanned changes, or the risk associated malware infections.

Briefly explaining, the key benefits of Control Compliance Suite Virtualization Security Manager are as the following:

- Virtual assets are secured against both the internal and the external threats
- By managing privileged accounts and access rights, the risk and security posture is improved
- It reduces the compliance scope, and this is done by effective isolation of impacted virtual environments/systems
- It reduces risk

To summarize, the main features of the Control Compliance Suite Virtualization Security Manager are as the following:

- The instances of the virtual machine are logically separated
- It has granular access control mechanisms
    - Avoids misuse of privileged accounts
    - Manage access rights
- It has an effective and detailed logging mechanism
- It has a two-level approval cycle for key function protection.

3.4.3 Oracle Identity Manager

As discussed earlier, the growth of IT has been explosive. Moreover, due to the increased network communications and mobile computing needs, enterprises have the challenge of determining what resources are accessed by which users and for what purpose they should be accessed. In fact, it is important to be aware of access management in a comprehensive manner. It is also important to impose governance controls for reducing the risk associated with access rights. A poor access management might lead to malicious act of any user of the system. This user could be the employee, contractor, etc. It is also essential to meet the legal requirements. Without an appropriate access controls, it will be challenging for the enterprise to provide adequate evidence to the testers of the IT environment (Oracle Identity Manager - Business Overview, 2014).

In fact, it is a challenging task for many enterprises to enforce governance controls for access management. Generally, more users are getting involved in driving governance initiatives, such as requesting access or delegate administrating activities. Therefore, in order to have successful and effective enterprise governance, a critical requirement would be having a simple, user friendly and customizable tool.

Oracle Identity Governance Suite can provide benefits like:

- Increasing end-user productivity
- Reducing risk
- Increasing operational efficiency
- Reducing total cost.

Since, the focus of the thesis is on IT controls testing, the concentration will be on testing/auditing features. The Oracle Identity Manager has two main testing related capabilities. First, it has the capability to enforce IT audit policy; second, it has reporting and auditing capabilities.

In Oracle Identity Manager, an engine is managing the assignment of privileges and entitlements to users. Hence, it must ensure that users are assigned to intended roles, with specified and controlled privileges, in such a way that they do not end up in a situation where they are able to commit fraud. In fact, the access to the IT systems is governed by IT Audit policies. The IT Audit policies define preventive measures for the users, in such a way that they are not able to acquire entitlements that are in compliance with the enterprise's policies. For instance, if the IT Audit policies are not in use, it is possible that a user generates and approves invoices without being noticed. Perhaps, IT Audit Policy tries to ensure that a user does not have rights to perpetrate a fraud.

Oracle Identity Manager includes provisioning functions that ensure enterprises are IT Audit Policy compliant. This compliance is obtained through various means; pre-provisioning and real-time validation IT Audit Policy engine, the engine that manages the Audit policies for the applicable applications. And to (Oracle Identity Manager - Business Overview, 2014) **"***This is done through an integration framework that allows the business to plug Oracle Identity Manager into leading IT Audit policy engines such as Oracle Application Access Controls Governor and SAP GRC Access Controls."*

3.5 Result of Analysis; Developing IT Controls Testing

Analysis of some the existing CAAT tools (Bwise Internal Audit Software, Oracle Enterprise GRC Manager – Fusion Edition, ServiceNow IT Governance, Risk and Compliance, Symantec Control Compliance Suite Vendor Risk Manager, Symantec Control Compliance Suite Virtualization Security Manager, and Oracle Identity Manager) is completed in the previous sections. In fact, these CAAT tools are popular and widely used in many enterprises across the world.

After analysis of the existing CAAT tools, crucial information is obtained. In actuality, understanding each and every aspect of the existing CAAT tools is a very crucial factor for developing IT controls testing.

One main clear conclusion of this analysis is that these enterprise widely used CAAT tools are capable of performing specific tasks. As a matter of fact, the existing CAAT tools are having the capability to audit only certain systems. Moreover, each of these tools is capable of addressing certain number of controls. No one existing CAAT tool is

having the capability to check all the important aspects of an enterprise IT environment. For instance, the existing CAAT tools are developed in such a way that they are concentrating on specific IT controls. Whereby, for an ideal and appropriate IT controls testing it would be best to have a tool that could test the whole IT environment without focusing only on a particular area, in other words, it would have ideal to have a CAAT tool that could focus on all the controls.

In order to address the challenge that existing CAAT tools are in capable of focusing on all the areas of an enterprise's IT environment, one assumption could be using different CAAT tools, so that almost the whole IT environment could be tested. But the strong argument that will support the infeasibility of this assumption is the high cost of such tools. Actually, for almost all the enterprises, it is not possible to invest a very huge capital for purchasing several IT CAAT tools. Furthermore, even for many enterprises, purchasing a single CAAT tool is considered to be a challenge. Therefore, the idea of using several CAAT tools for meeting the requirements of the business is more or less against the business requirements flow.

It could be assumed that since handling of internal and external threats is of great concern for the enterprises, the required capital would be invested for purchasing several CAAT tools for facilitating IT controls testing for the whole enterprise's IT environment. Now the challenge would be the work effort and skills required for handling the various CAAT tools. The whole process of IT controls testing is already expensive, and hiring skilled employees with the capability of working with the different CAAT tools or training the existing employees, would require huge amount of time and money. As a result, even if the capital for purchasing various CAAT tools is provided, still running the whole process would be extremely expensive. Therefore, it can be concluded that the use of various CAAT tools is not at all a solution for an ideal or at least close to ideal IT controls testing.

Another conclusion achieved from analyzing the existing CAAT tools is the ignorance/inappropriate use of the existing ERP data. If a CAAT tool could have the capability of using the existing ERP data in an appropriate way, it would make the job of the tester/auditor much simpler, it would require less human intervention, it would reduce the cost of auditing, it wouldn't require many CAAT tools to facilitate IT controls testing, it wouldn't require a number of employees with different technical backgrounds and skills. Most importantly, by relying on the existing ERP data, the controls could be tested in an accurate manner.

But using the existing ERP data by the CAAT tool(s) for the purpose of IT controls testing has its own challenges. It is should be kept in mind that the quality of the existing ERP data is very important. And this is because the result of the testing highly depends on the quality of the existing ERP data. Therefore, it is correct to state that it would be ideal to perform IT controls testing with a high quality existing ERP data.

When the quality of the existing ERP data is of concern, it should be considered that the data should be coherent. If the data is not coherent enough, enterprise using that data is highly prone to consequences. For instance, if the pulled out data is not coherent and is not right, therefore, the result of the testing is definitely wrong. Consider a scenario that wrong data is retrieved for analysis, then the result of the testing indicates that a particular system is not functioning in accordance with the requirements, whereby, the system is completely okay. Or considering the opposite scenario, where right data is pulled out, but due to lack of coherence, the result indicates that the IT systems are functioning appropriately, whereby, the systems, or at least some of them might not run appropriately. The result of both the scenarios would lead to extreme consequences for the enterprise.

Therefore, when testing the IT environment of an enterprise with a CAAT tool that uses the existing ERP data of the enterprise, the quality of the data must be checked and tested. Moreover, data must be measured and analyzed. In addition, the use of existing ERP data by the CAAT tool, requires automated procedure, but prior to automation, data must be analyzed. And this is because; right data must be measured, analyzed and embedded into an automated process so that right data, for right process is deployed.

In addition to the challenges of using existing ERP data such as data quality and data coherence, developing a data structure for the purpose of mapping the data to the CAAT tool is another challenge. It is not feasible to have a standard format data structure that can map data of the enterprises to a CAAT tool, in such a way that it covers all the IT controls of all the enterprises.

Therefore, for developing IT controls testing, developed CAAT tools required. In fact, CAAT tools that is capable of using inherited data from the IT systems of an enterprise. In addition, such tools should have the capability of measuring data and analyzing it, for checking the quality and coherence of data, mapping the data to automated functions, and producing accurate and accountable results in a real time manner.

4. CONCLUSIONS

At this point, it has been observed that the speed and range of development of IT is increasing at a high rate. More and more enterprises are increasing their dependency on IT. And this enormous IT ecosystem is highly prone to internal and external threats. Therefore, for any enterprise which is willing to meet its business objectives, internal and external threats must be detected, prevented or mitigated. The enterprises need to focus on the avoiding or decreasing the impact of such threats on their IT environment, which is in tight relationship with business environment.

For this reason, many enterprises have already comprehended the importance of IT controls testing. It is realized that an appropriate IT controls testing tries to ensure that IT environment of an enterprise is aligned with the business objectives of the enterprise. It has been noted that an appropriate IT controls testing helps to detect the internal and external threats to the enterprise, and to prevent/mitigate the impact of those threats. Thereby, this helps the enterprises to have a qualitative service delivery, better performance, efficient use of IT resources, and achieving the business objectives.

In addition, it has been also understood that several components are playing key role for the process IT controls testing. Several procedures, processes, tools, etc., have vital role in IT controls testing.

It has been also noted that even though plenty of CAAT tools with plenty of promises exist, but still the task of IT controls testing is not conducted in an appropriate method by relying only on the existing CAAT tools, due to their analyzed weaknesses. Therefore, expensive CAAT tools, costly skilled employees, reliable framework and standards, external auditors, etc., are not the perfect and final solution for an effective, efficient and reliable IT controls testing.

In addition, it has been observed that even though if the necessary CAAT tools are deployed, the highly skilled employees are available, and industry best practices are in place, still the process of IT controls testing is highly expensive, it requires a huge amount of manual effort, it requires cumbersome configurations, and still it does not meet the criteria of an ideal It controls testing.

Hence, appropriate and ideal use of existing ERP data is highly required by an enterprise for IT controls testing. Appropriate existing ERP data is the data that measured appropriately, analyzed appropriately, mapped and automated by the CAAT tools appropriately. In fact, it is a challenging task for an enterprise to develop its IT controls

testing to such level, where the IT controls testing is done with lower cost, in real-time, with less human intervention, i.e. work effort, and higher frequency is challenging. But if the development is made to the process in a way that the requirement for multiple tools does not exist by simply putting more effort into proper use of existing ERP data, an ideal IT controls testing is feasible.

In conclusion, it might be correct that implementing such an IT controls testing process is complex, and maybe even expensive, but if implementing such a system in an enterprise environment does not require to be repeated on yearly basis, then in the long run the enterprise will be benefited from a system that exclude challenges, such as cost, work effort, frequency of testing, accuracy, etc. And as the reliability of the IT controls testing increases, the reliability of the IT environment increases as well, as a result, the impact of risks associated with IT environment diminishes or even avoided. Therefore, an enterprise could meet the business objectives by depending on the plenty of benefits that IT provides.

REFERENCES

Adams, S.;Ruiz, C.;& Rivera, E. (May 2013). *ISACA.* Retrieved from Governance, Risk and Compliance ISACA Monterrey: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20132305%20Governance,%20Risk%20and%20Compliance.pdf

Bidgoli, H. (2004). *The Internet Encyclopedia.* John Wiley & Sons.

Breaux, T.D.; Anton, A.I.; Boucher, K.; Dorfman, M., "IT Compliance: Aligning Legal and Product Requirements," *IT Professional* , vol.11, no.5, pp.54,58, Sept.-Oct. 2009
doi: 10.1109/MITP.2009.101
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5271537&isnumber=5271519

BWise. (2014). *About BWise.* Haettu 11. Octtober 2014 retrieved BWise: http://www.bwise.com/about-bwise#.VDOMpPmSzkV

Zhixiong Chen; Jong Yoon; Frenz, C.M.; Compres, K., "IT Governance, Compliance and Auditing Curriculum--A Pedagogical Perspective," *Services (SERVICES), 2011 IEEE World Congress on* , vol., no., pp.414,421, 4-9 July 2011
doi: 10.1109/SERVICES.2011.87
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6012768&isnumber=6012651

Control Compliance Suite Virtualization Security Manager. (October 2012). Haettu 9. October 2014 retrieved from Symantec Corporation: javascript:trackDownloadFileOpen('/content/en/us/enterprise/fact_sheets/b-ccs_virtualization_security_manager_DS_21274408.en-us.pdf');

COSO. (2013). Internal Control - Integrated Framework. Teoksessa *Internal Control - Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

(2014). *Data Breach Investigation Report.* Verizon. retrieved from file:///C:/Users/k765343/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf

Ginzberg, M.J.; Moulton, R.T., "Information technology risk management," *Information Technology, 1990. 'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on (Cat. No.90TH0326-9)* , vol., no., pp.602,608, 22-25 Oct 1990
doi: 10.1109/JCIT.1990.128338
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=128338&isnumber=3595

Hanna, A. (May 2011). *ITIL Glossaries.* Haettu 28. October 2014 retrieved ITIL: http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.* Mc-Graw Hill.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security technical Report 13*, (pp. 247 - 255)

Hussain, S.J.; Siddiqui, M.S., "Quantified Model of COBIT for Corporate IT Governance," *Information and Communication Technologies, 2005. ICICT 2005. First International Conference on* , vol., no., pp.158,163, 27-28 Aug. 2005
doi: 10.1109/ICICT.2005.1598575
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1598575&isnumber=33619

IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition. (2006). IT Governance Institute.

IT Governance Institute. (2007). *COBIT 4.1.* Illinois: IT Governance Institute.

Key Benefits of ITIL. (ei pvm). Haettu 28. October 2014 retrieved ITIL: http://www.itil-officialsite.com/key-benefits/key-benefits-itil.aspx

Khosrowpour, M. (2006). *Emerging Trends and Challenges in Information Technology Management.* Idea Group Inc. (IGI).

Krey, M.; Harriehausen, B.; Knoll, M., "Approach to the Classification of Information Technology Governance, Risk and Compliance Frameworks," *Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on* , vol., no., pp.350,354, March 30 2011-April 1 2011 doi: 0.1109/UKSIM.2011.73
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5754240&isnumber=5754186Kushner, D. (26. February 2013). *The Real Story of Stuxnet*.

IEEE Spectrum: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Lamm, J.;& Zanella, R. (2010). *Under Control; Governance Across the Enterprise.* New York: CA Press.

Long, J. (2008). *ITIL Version 3 at a Glance.* Springer.

Niemann, K. D. (2006). *From Enterprise Architecture to IT Governance.* Vieweg.

Oracle. (2009). *Enterprise GRC Manager.* Haettu 12. October 2014 retrieved Oracle: http://www.oracle.com/us/solutions/corporate-governance/risk-financial-governance/enterprise-GRC-manager/overview/index.html

Oracle Identity Manager - Business Overview. (January 2014). Haettu 13. October 2014 retrieved Oracle: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.oracle.com%2Ftechnetwork%2Fmiddleware%2Fid-mgmt%2Foverview%2Foig-11gr2-ps1-business-wp-1928896.pdf&ei=ClpXVMWaKNPraOW_gfAN&usg=AFQjCNEezaa6WcI

Parvizi, R.; Oghbaei, F.; Khayami, S.R., "Using COBIT and ITIL frameworks to establish the alignment of business and IT organizations as one of the critical success factors in ERP implementation," *Information and Knowledge Technology (IKT), 2013 5th Conference on* , vol., no., pp.274,278, 28-30 May 2013
doi: 10.1109/IKT.2013.6620078

URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6620078&isnumber=6620027

Pathak, J. (2005). *Information Technology Auditing.* Berlin: Springer.

PriceWaterhouseCoopers. (2014). *US cybercrime: Rising risks, reduced readiness.* PriceWaterhouseCoopers (PwC).

ProQuest. (2014). *Report Information from ProQuest.* Coventry: Close-Up Media, Inc.

Puspasari, D.; Hammi, M.K.; Sattar, M.; Nusa, R., "Designing a tool for IT Governance Risk Compliance: A case study," *Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on* , vol., no., pp.311,316, 17-18 Dec. 2011
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6140793&isnumber=6140728

PwC. (2008). *Integrated Governance, Risk and Compliance.* Haettu 28. October 2014 retrieved PriceWaterhouseCoppers:

https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCYQFjAB&url=https%3A%2F%2Fwww.pwc.com%2Fen_US%2Fus%2Fpublic-sector%2Fassets%2Ffederal_igrc.pdf&ei=EkxPVOv0EqP5yQPOx4GwBw&usg=AFQjCNEzNMMvBIwQB8hVqDVSUqRYrDkOVg&bvm=bv.7788

Racz, N.; Weippl, E.; Bonazzi, R., "IT Governance, Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study," *Services (SERVICES), 2011 IEEE World Congress on* , vol., no., pp.429,436, 4-9 July 2011
doi: 10.1109/SERVICES.2011.78,
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6012770&isnumber=6012651

Radovanović, D.; Radojević, T.; Lučić, D.; Sarac, M., "IT audit in accordance with Co-bit standard," *MIPRO, 2010 Proceedings of the 33rd International Convention* , vol., no., pp.1137,1141, 24-28 May 2010
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533627&isnumber=5533310

Rouse, M. (August 2014). *ERP (enterprise resource planning)*. Haettu 28. October 2014 retrieved TechTarget: http://searchsap.techtarget.com/definition/ERP

S.H.Hong. (2011). *Strategy for Strenthening Financial IT Internal Control.* Financial Security Agency.

SAP Enterprise Resource Planning (ERP). (2013). Haettu 28. October 2014 retrieved Izon Systems: http://www.izonsystems.co.ke/images/ERP-Graphic.jpg

Sawyer, L. (2012). *Sawyer's Guide for Internal Auditors, 6th Edition.* The IIA Research Foundation.

Sayana, S. (2003). Using CAATs to Support IS Audit. *Information Systems Control Journal, Volume 1*.

Schultz, M.;Ruehle, A.;& Gehrke, N. (2014). Audit-focused mining - New Views on Integrating Process Mining and Internal Control. *ISACA Journal Volume 3*.

Securities and Exchange Commisions. (2007). *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934.* Washington: Securities and Exchange Commission (SEC).

ServiceNow. (2014). *About ServiceNow*. Haettu 10. October 2014 retrieved ServiceNow: http://www.servicenow.com/company.html

ServiceNow IT Governance, Risk and Compliance. (2014). Haettu 10. October 2014 retrieved ServiceNow: http://www.servicenow.com/products/it-governance-risk-and-compliance.html

Symantec Control Compliance Suite. (ei pvm). Haettu 12. October 2014 retrieved Symantec Corporation: http://www.symantec.com/control-compliance-suite

Symantec Control Compliance Suite. (April 2014). Haettu 10. October 2014 retrieved Symantec Corporation: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-symc-control-compliance-suite-vendor-risk-mgr-DS-2128940.pdf

What is ITIL? (ei pvm). Haettu 28. October 2014 retrieved ITIL: http://www.itil-officialsite.com/aboutitil/whatisitil.aspx

Vicente, P.; da Silva, M.M., "A Business Viewpoint for Integrated IT Governance, Risk and Compliance," *Services (SERVICES), 2011 IEEE World Congress on* , vol., no., pp.422,428, 4-9 July 2011
doi: 10.1109/SERVICES.2011.62
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6012769&isnumber=6012651

Williams, R. (22. May 2014). *The biggest ever cyber attacks and security breaches*. Retrieved from The Telegraph: http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggest-ever-cyber-attacks-and-security-breaches.html

Zhong Yao; Xin Wang, "An ITIL based ITSM practice: A case study of steel manufacturing enterprise," *Service Systems and Service Management (ICSSSM), 2010 7th International Conference on* , vol., no., pp.1,5, 28-30 June 2010
doi: 10.1109/ICSSSM.2010.5530204
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5530204&isnumber=5530078

Young Rok Yu; Seong Chae Seo; Byung Ki Kim, "IT GRC-based IT internal control framework," *Advanced Communication Technology (ICACT), 2013 15th International Conference on* , vol., no., pp.382,385, 27-30 Jan. 2013
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6488211&isnumber=6488107